FAST TURN AROUND

quotes@ftainsurance.com.au
ftainsurance.com.au
(02) 9003 1660

Claim Focus

Information Technology (IT)

Background:

An Insured was engaged to provide Information Technology (IT) services to its client, including the management and maintenance of the client's telephony systems.

Incident:

In January 2026, following system testing of the client's telephony platform, the multi-factor authentication (MFA) was not re-enabled. This security lapse allowed an unknown third party to gain unauthorised access to the system.

As a result, a huge number of unauthorised international calls were made through the client's telephony network, leading to significant excess call charges imposed by the telecommunications provider.

Why do "hackers" do this:

International Revenue Sharing Fraud (IRSF): Hackers break into a company's phone (VoIP) system and use it to automatically call premium-rate international numbers that they own or control.

Reselling Stolen Minutes: The hacker essentially uses the client's telephony network as a free, unlimited phone carrier. They sell heavily discounted international calling services or "phone cards" to unsuspecting third parties on the dark web. Since the client's network foots the bill, the hacker keep 100% of the profits from the sale.

Key Takeaways for Brokers:

- **Early engagement and full cooperation** from the Insured can significantly improve claim outcomes and preserve client relationships.
- **Accurate incident timelines** are crucial in determining causation and quantifying loss.
- **IT Liability policies** can respond to third-party financial loss arising from service errors, where a clear causal link is established.
- Consider whether a **Cyber Policy** may also respond in similar scenarios involving unauthorised acces or security breaches.

Contact Us:

Hansini Seenuth

Claims Officer

(03) 8525 0127

claims@ftainsurance.com.au

Claim Focus (cont.)

Information Technology (IT)

Quantum:

The Insured provided to FTA all supporting documentation, including summary of incurred charges, Incident report, invoices issued by the telecommunications provider (TFL) for the period 1 January 2026 to 28 February 2026. The total claimed loss amounted to **$234,031.04**.

Policy Response:

The Insured sought out indemnity under **Clause 1.1 - Professional Liability** of their IT Liability Policy, which provides cover for civil liability arising from claims connected with:

- The performance of Information Technology Services; or
- The provision of Information Technology Products

The circumstances were considered to fall within policy coverage, subject to terms and conditions.

Liability Assessment:

Investigations identified that the failure to reinstate MFA following testing constituted an error in the provision of IT services. This created a foreseeable vulnerability, which directly led to the unauthorised access and resulting financial loss. Accordingly, there was a reasonable basis to attribute liability to the Insured

Resolution:

Both the Insured and the client were motivated to resolve the matter promptly, given their ongoing relationship. FTA's claims handlers worked with the Insured and the Claimant to quickly finalise the matter.

Key Takeaways for Brokers:

- **Early engagement and full cooperation** from the Insured can significantly improve claim outcomes and preserve client relationships.
- **Accurate incident timelines** are crucial in determining causation and quantifying loss.
- **IT Liability policies** can respond to third-party financial loss arising from service errors, where a clear causal link is established.
- Consider whether a **Cyber Policy** may also respond in similar scenarios involving unauthorised acces or security breaches.

Contact Us:

Hansini Seenuth

Claims Officer

(03) 8525 0127

claims@ftainsurance.com.au